平泉町教育情報セキュリティポリシー

令和８年３月

平泉町教育委員会

目次

序　平泉町教育情報セキュリティポリシーについて

平泉町教育情報セキュリティポリシーは、本町が保有する教育情報資産に関する教育情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものである。

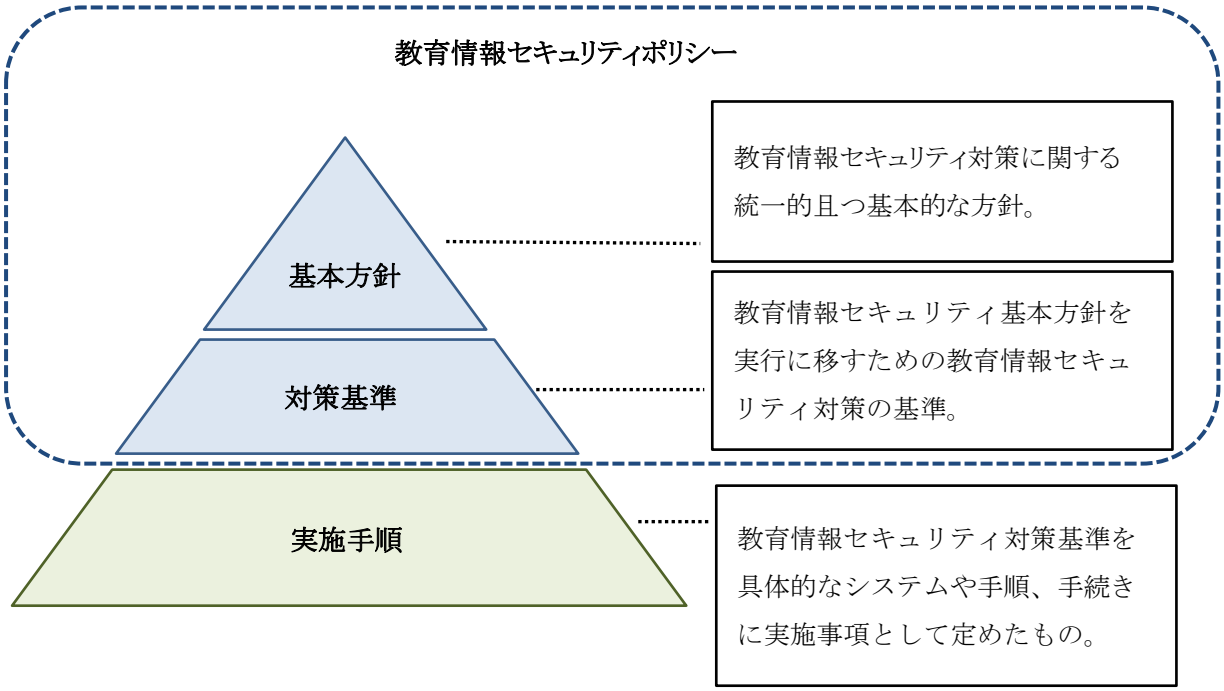
この教育情報セキュリティポリシーの目的は、教育情報セキュリティを確保するための考え方、体制、運用等を規定することによって業務の安定的な運用を図ること、そして本町が保有する個人情報、教育情報資産を守ることである。

教育情報セキュリティポリシーは、本町が教育情報セキュリティに対する基本的な考え方を示した「平泉町教育情報セキュリティ基本方針」と、その基本方針に基づいたセキュリティ対策の基準を定める「平泉町教育情報セキュリティ対策基準」の２階層に分けて策定する。これらは、常に水準の向上を図るため、継続的な評価・見直しを実施する。

そして、「平泉町教育情報セキュリティ基本方針」及び「平泉町教育情報セキュリティ対策基準」に基づき、各情報システムの具体的な情報セキュリティ対策の実施手順を策定することとする。

なお、本書の対象とする範囲は、「平泉町教育情報セキュリティポリシー」を構成する「平泉町教育情報セキュリティ基本方針」と「平泉町教育情報セキュリティ対策基準」であり、「実施手順」は含まれない。

【教育情報セキュリティポリシーの構成】



第１章　情報セキュリティ基本方針

1. 目的

本基本方針は、本町が保有する教育情報資産の『機密性』、『完全性』、『可用性』を維持するために、本町が実施する教育情報セキュリティ対策について、基本的な事項を定めることを目的とする。

2. 定義

この訓令において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

（１）ネットワーク　コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（２）情報システム　コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（３）記録媒体　電子計算機に使用される電子的方式、磁気的方式又は光学的方式その他人の知覚によっては認識することができない方式で作られたデータを記録するための機器媒体をいう。

（４）情報セキュリティ　情報資産の機密性、完全性及び可用性を維持することをいう。

（５）情報資産　ネットワーク及び情報システムで取り扱うすべての情報をいう。
（ネットワーク及び情報システムに関する設備、記録媒体、印刷物も含む）

（６）機密性　情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（７）完全性　情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（８）可用性　情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（９）教育情報セキュリティポリシー　本基本方針及び教育情報セキュリティ対策基準をいう。

（１０）教育情報セキュリティ基本方針　教育情報セキュリティを維持する方策に関する根本的な事項を定めたものをいう。

（１１）教育情報セキュリティ対策基準　教育情報セキュリティ基本方針に基づき、情報セキュリティの維持のために遵守すべき行為及び判断を示したものをいう。

（１２）教育情報セキュリティ実施手順　教育情報セキュリティ対策基準に基づき、教育情報システム及びこれを使用する業務において、どのような手順を実行していくかを示したものをいう。

（１３）校務系情報　学校が保有する情報資産のうち、それらの情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報をいう。

（１４）学習系情報　学校が保有する情報資産のうち、それらの情報を学校における教育活動において活用することを想定しており、かつ、当該情報に教員及び児童生徒がアクセスすることが想定されている情報をいう。

（１５）校務用端末　校務系情報にアクセス可能な端末をいう。

（１６）学習者用端末　学習系情報にアクセス可能な端末で、児童生徒が利用する端末をいう。
（１７）指導者用端末　学習系情報にアクセス可能な端末で、教員のみが利用可能な端末をいう。
（１８）端末　校務用端末、学習者用端末及び指導者用端末の総称をいう。
（１９）校務系システム　校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム及び、校務系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステムをいう。
（２０）学習系システム　学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム及び、学習系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステムをいう。
（２１）教育情報システム　校務系システム及び学習系システムを合わせた総称をいう。
（２２）校務系サーバ　校務系情報を取り扱うサーバをいう。
（２３）学習系サーバ　学習系情報を取り扱うサーバをいう。
（２４）教育ネットワーク　教育情報資産を扱う通信回線、ルータ等の通信機器をいう。
（２５）クラウド　施設外データセンター等でプログラムやデータベースを管理し、ネットワークを介してこれを利用する仕組みや概念をいう。
（２６）ソーシャルメディアサービス　インターネット上における、ホームページ、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等をいう。
（２７）不正アクセス　不正アクセス行為の禁止等に関する法律(平成 11 年法律第 128 号)第 3 条第 2 項各号に規定する行為をいう。
（２８）不正操作　正規のアクセス権を持たない人が、意図する意図しないにかかわらず本来の目的以外及び手法でコンピュータを利用することをいう。
（２９）ウィルス　他人のコンピュータに勝手に入り込み、不具合を生じさせるプログラムをいう。
（３０）インターネット接続系　インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。
（３１）無害化通信　インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

3. 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。
（1）不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等
（2）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、

プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（3）地震、落雷、火災等の災害によるサービス及び業務の停止等

（4）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（5）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4. 適用範囲

この訓令の対象範囲は、次のとおりとする。

（1）行政機関の範囲　対象となる組織は、平泉町のすべての執行機関、議会事務局及び公営企業(以下「町等」という。)とする。また、対象となる者は、町等の情報資産を取り扱うすべての職員（非常勤職員及び会計年度任用職員等を含む）、契約に基づき情報資産を取り扱う外部委託業者その他の者(以下「職員等」という。)とする。

（2）情報資産の範囲

本基本方針が対象とする情報資産は、 次のとおりとする。

①教育ネットワーク、教育情報システム及びこれらに関する設備、 電磁的記録媒体

②教育ネットワーク及び教育情報システムで取り扱う情報

（これらを印刷した文書を含む。）

③教育情報システムの仕様書及びネットワーク図等のシステム関連文書

5. 職員等の遵守義務

職員等（職員、非常勤職員及び会計年度任用職員等をいう。以下同じ。）は、教育情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって教育情報セキュリティポリシー及び教育情報セキュリティ実施手順を遵守するものとする。

6. 教育情報セキュリティ対策

第3の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（1）組織体制　町の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（2） 教育情報資産の分類と管理　町の保有する教育情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき教育情報セキュリティ対策を実施する。

（3） 情報システム全体の強靭性の向上　インターネットを介した教育情報資産へのアクセスにおいては、クラウド利用も含め、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

（4） 物理的セキュリティ　　サーバ等、情報システム室等、通信回線等及び職員等が利用する端末等の管理について、物理的な対策を講じる。

（5）人的セキュリティ　　情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（6） 技術的セキュリティ　　端末やサーバ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（7） 運用　　情報システムの監視、教育情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、教育情報セキュリティポリシーの運用面の対策を講じるものとする。 また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、情報セキュリティインシデント対応要領を策定する。

（8）外部サービスの利用　外部委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（9）評価・見直し　　教育情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い情報セキュリティの向上を図る。 情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

7. 情報セキュリティ監査及び自己点検の実施

教育情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8. 教育情報セキュリティポリシーの見直し

教育情報セキュリティ監査及び自己点検の結果、教育情報セキュリティポリシーの見直しが必要となった場合及び教育情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、教育情報セキュリティポリシーを見直す。

9. 教育情報セキュリティ対策基準の策定

６、 ７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める教育情報セキュリティ対策基準を策定する。

10. 教育情報セキュリティ実施手順の策定

教育情報セキュリティ対策基準に基づき、教育情報セキュリティ対策を実施するための具体的な手順を定めた教育情報セキュリティ実施手順を策定するものとする。

なお、教育情報セキュリティ実施手順は、公にすることにより町の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。